(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 December 2000 (28.12.2000)

PCT

(10) International Publication Number
WO 00/79434 A1

(51) International Patent Classification[7]: G06F 17/30

(21) International Application Number: PCT/US00/17078

(22) International Filing Date: 21 June 2000 (21.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/140,417 22 June 1999 (22.06.1999) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US PCT/US99/1485 (CIP)
Filed on 28 June 1999 (28.06.1999)

(71) Applicant *(for all designated States except US)*: INTERNET DYNAMICS, INC. [US/US]; 3717 E. Thousand Oaks Boulevard, Westlake Village, CA 91362 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: HANNEL, Clifford, Lee [US/US]; 3178 Futura Point, Thousand Oaks, CA 91362 (US). MAY, Anthony, Allan [CA/US]; 6644 Glade Avenue #217, Woodland Hills, CA 91303 (US).

(74) Agent: NELSON, Gordon, E.; 57 Central Street, P.O. Box 782, Rowley, MA 01969 (US).

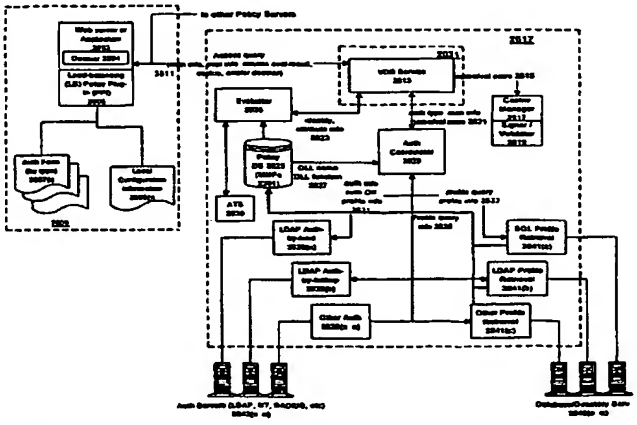
(81) Designated States *(national)*: AU, JP, SG, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: QUERY INTERFACE TO POLICY SERVER



(57) Abstract: A scalable access filter that is used together with others like it in a virtual private network to control access by users at clients in the network to information resources provided by servers in the network. Each access filter use a local copy of an access control data base (3845) to determine whether an access request is made by a user. Each user belongs to one or more user groups and each information ressource belongs to one or more information sets. Access is permitted or denied according to access policies which define access in terms of the user groups and information sets. The first access filter in the path performs the access check, encrypts and authenticates the request; the other access filters in the path do not repeat the access check. The interface used by applications to determine whether a user has access to an entity is now an SQL query. The policy server (3811) assembles the information needed for the response to the query from various information sources, including source external to the policy server.

WO 00/79434 A1